UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/370,384	08/09/1999	DANIEL F. ZUCKER	M-7190-US	8054

24251 7590 06/06/2003

SKJERVEN MORRILL LLP
25 METRO DRIVE
SUITE 700
SAN JOSE, CA 95110

EXAMINER	
SMITHERS, MATTHEWS	

ART UNIT	PAPER NUMBER
2134	3

DATE MAILED: 06/06/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/370,384	ZUCKER, DANIEL F.	
	Examiner	Art Unit	
	Matthew B Smithers	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 August 1999* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-9,13,15-17 and 21-24* is/are rejected.

7)☒ Claim(s) *3,10-12,14,18-20,25 and 26* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 4-9, 13, 15-17, and 21-24 rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. patent 6,330,671 granted to Aziz and further in view of U.S. patent 6,041,408 granted to Nishioka et al.

Regarding claim 1, Aziz teaches a method for secure key management in a multicast network where a requesting node (first recipient) is authenticated by a seed node (security server) to determine if the requesting node has permission to receive a cryptographic key (set of encrypted bits) (see column 8, line 12 to column 9, line 64). Aziz further teaches the requesting node can broadcast to a plurality of receivers after receiving the multicast key (see column 11, lines 37-44). Aziz fails to specifically teach transmitting a subset of encrypted bits for generating a set of encryption bits (key) at the first recipient (requesting node). Nishioka teaches a key distribution method in a secure broadcast communication where a subset of encrypted bits are used to generate key information (see Abstract and column 5, lies 28-62). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Aziz' method for secure key distribution in a multicast network with Nishioka's method for

secure broadcast communication in order to efficiaently reduce the length of key distribution data transmitted without compromising confidential information in the system [see Nishioka et al; column 2, lines 50-59].

Regarding claim 2, Aziz and Nishioka et al disclose everything claimed as applied above (see claim 1), in addition Aziz teaches a time stamp (see column 11, lines 30-34).

Regarding claim 4, Aziz and Nishioka et al disclose everything claimed as applied above (see claim 1), in addition Aziz teaches transmitting an identification of the first recipient to said security server and comparing said identification to said access information to establish authentication when said identification matches said access information (see column 8, lines 47-64).

Regarding claim 5, Aziz and Nishioka et al disclose everything claimed as applied above (see claim 1), in addition Aziz teaches transmitting a set of encrypted bits (key) from a first receiver to said security server; authenticating said first receiver at said security server; transmitting a second set of bits from said security server to said first receiver if said first receiver is authenticated (see column 11, lines 17-63).

Regarding claim 6, Aziz and Nishioka et al disclose everything claimed as applied above (see claim 1), in addition Nishioka teaches attaching an offset value (see column 15, lines 53-56).

Regarding claim 7, Aziz and Nishioka et al disclose everything claimed as applied above (see claim 1), in addition Aziz teaches memory for storing (see column 7, lines 13-18).

Regarding claim 8, Aziz and Nishioka et al disclose everything claimed as applied above (see claim 7), in addition Aziz teaches memory for storing (see column 6, line 58 to column 7, line 1).

Regarding claim 9, Aziz and Nishioka et al disclose everything claimed as applied above (see claim 8), in addition Aziz teaches returning a stored set of encrypted bits (key) from said memory if said set of encrypted bits matches said stored set of encrypted bits (see column 6, line 58 to column 7, line 1).

Regarding claim 13, Aziz and Nishioka et al disclose everything claimed as applied above (see claim 1), in addition Aziz teaches broadcasting datagrams (data packets) (see column 9, lines 44-64).

Regarding claim 15, Aziz teaches a method for secure key management in a multicast network where a requesting node (first recipient) is authenticated by a seed node (security server) to determine if the requesting node has permission to receive a cryptographic key (set of encrypted bits) (see column 8, line 12 to column 9, line 64). Aziz further teaches the requesting node can broadcast to a plurality of receivers after receiving the multicast key (see column 11, lines 37-44). Aziz fails to specifically teach transmitting a subset of encrypted bits for generating a set of encryption bits (key) at the first recipient (requesting node). Nishioka teaches a key distribution method in a secure broadcast communication where a subset of encrypted bits are used to generate key information (see Abstract and column 5, lies 28-62) and Nishioka teaches attaching an offset value (see column 15, lines 53-56). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Aziz' method for

secure key distribution in a multicast network with Nishioka's method for secure broadcast communication in order to efficiaently reduce the length of key distribution data transmitted without compromising confidential information in the system [see Nishioka et al; column 2, lines 50-59].

Regarding claim 16, Aziz teaches a method for secure key management in a multicast network where a requesting node (first recipient) is authenticated by a seed node (security server) to determine if the requesting node has permission to receive a cryptographic key (set of encrypted bits). The cryptographic key is enclosed in a certificate (seal) (see column 8, line 12 to column 9, line 64). Aziz further teaches the requesting node can broadcast to a plurality of receivers after receiving the multicast key (see column 11, lines 37-44). Aziz fails to specifically teach transmitting a subset of encrypted bits for generating a set of encryption bits (key) at the first recipient (requesting node). Nishioka teaches a key distribution method in a secure broadcast communication where a subset of encrypted bits are used to generate key information (see Abstract and column 5, lies 28-62). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Aziz' method for secure key distribution in a multicast network with Nishioka's method for secure broadcast communication in order to efficiaently reduce the length of key distribution data transmitted without compromising confidential information in the system [see Nishioka et al; column 2, lines 50-59].

Regarding claim 17, Aziz and Nishioka et al disclose everything claimed as applied above (see claim 16), in addition Aziz teaches returning a permit (key)

corresponding to a first previously opened seal from said memory if said seal matches said first previously opened seal (see column 6, line 58 to column 7, line 1).

Regarding claim 21, Aziz teaches a method for secure key management in a multicast network where a requesting node (first recipient) is authenticated by a seed node (security server) to determine if the requesting node has permission to receive a cryptographic key (set of encrypted bits). The cryptographic key is enclosed in a certificate (seal) (see column 8, line 12 to column 9, line 64). Aziz further teaches the requesting node can broadcast to a plurality of receivers after receiving the multicast key (see column 11, lines 37-44) and broadcast datagrams (data packets) (see column 9, lines 44-64). Aziz fails to specifically teach transmitting a subset of encrypted bits for generating a set of encryption bits (key) at the first recipient (requesting node). Nishioka teaches a key distribution method in a secure broadcast communication where a subset of encrypted bits are used to generate key information (see Abstract and column 5, lies 28-62). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Aziz' method for secure key distribution in a multicast network with Nishioka's method for secure broadcast communication in order to efficiaently reduce the length of key distribution data transmitted without compromising confidential information in the system [see Nishioka et al; column 2, lines 50-59].

Regarding claim 22, Aziz teaches a method for secure key management in a multicast network where a requesting node (first recipient) is authenticated by a seed node (security server) to determine if the requesting node has permission to receive a

cryptographic key (set of encrypted bits). The cryptographic key is enclosed in a certificate (seal) (see column 8, line 12 to column 9, line 64). Aziz further teaches the requesting node can broadcast to a plurality of receivers after receiving the multicast key (see column 11, lines 37-44). Aziz fails to specifically teach transmitting a subset of encrypted bits for generating a set of encryption bits (key) at the first recipient (requesting node). Nishioka teaches a key distribution method in a secure broadcast communication where a subset of encrypted bits are used to generate key information (see Abstract and column 5, lies 28-62). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Aziz' method for secure key distribution in a multicast network with Nishioka's method for secure broadcast communication in order to efficiaently reduce the length of key distribution data transmitted without compromising confidential information in the system [see Nishioka et al; column 2, lines 50-59].

Regarding claim 23, Aziz and Nishioka et al disclose everything claimed as applied above (see claim 22), in addition Aziz teaches transmitting said first seal from said second party to a security server; authenticating said second party at said security server; and transmitting a first permit from said security server to said second party if said second party is authenticated, said first permit being a subset of said first seal, in decrypted form, and containing information for encrypting/decrypting said first encrypted data stream (see column 8, line 12 to column 9, line 52).

Regarding claim 24, Aziz and Nishioka et al disclose everything claimed as applied above (see claim 23), in addition Aziz teaches generating a first set of

decryption bits at said second party; and decrypting said first encrypted data stream at said second party using said first set of decryption bits (see column 8, line 12 to column 9, line 52).

Allowable Subject Matter

Claims 3, 10-12, 14, 18-20, 25 and 26 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

For claim 3, The prior art of record fails to specifically teach the policy comprises information selected from the group consisting of security levels of said recipients and classification of said data stream.

For claims 10-12, and 18-20, The prior art of record fails to specifically teach when the set of encrypted bits fails to match any of said stored set of encrypted bits in said memory the application server further decrypts a set of encrypted bits at said security server to obtain access information and compares said identification of said receiver to said access information to establish authentication when said identification matches the access information.

For claim 14, The prior art of record fails to specifically teach appending said set of encrypted bits to said first encrypted data stream; and transmitting a second encrypted

data stream from said first receiver to said first recipient, wherein a second set of encrypted bits is appended to said second encrypted data stream.

For claims 25 and 26, The prior art of record fails to specifically teach transmitting a second seal from said first party to said security server; authenticating said first party at said security server; and transmitting a second permit from said security server to said first party if said first party is authenticated, said second permit being a subset of said second seal, in decrypted form, and containing information for encrypting/decrypting said second encrypted data stream.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Mittra (5,748,736) discloses a system for secure group communications via multicast or broadcast.

B. Caronni et al (6,195,751) discloses a secure multicasting network.

C. Wesley et al (6,275,859) discloses a tree based reliable multicast system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone

numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Matthew B Smithers
Primary Examiner
Art Unit 2134

June 1, 2003